

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples Vulnérabilités des produits CA

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-217>

Gestion du document

Référence	CERTA-2007-AVI-217
Titre	Multiples Vulnérabilités des produits CA
Date de la première version	11 mai 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité CA du 10 mai 2007
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- CA Anti-Virus for the Enterprise (eTrust Antivirus) version r8 et versions antérieures ;
- CA Threat Manager (eTrust Integrated Threat Management) version r8 et versions antérieures ;
- CA Anti-Spyware (eTrust PestPatrol) version r8 et versions antérieures.

3 Résumé

De multiples vulnérabilités ont été découvertes dans certains produits de la société CA. Ces vulnérabilités permettent à un utilisateur malintentionné de conduire des attaques par déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités ont été découvertes dans certains produits de la société CA :

- La première vulnérabilité résulte d'un débordement de tampon au niveau du traitement des identifiants. L'exploitation de cette vulnérabilité permet d'exécuter des commandes arbitraires à distance via le port 12168/TCP.
- La seconde faille est due à un débordement de tampon présent au niveau de la bibliothèque *InoCore.dll*. Cette vulnérabilité peut être exploitée localement afin d'élever ses privilèges.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de vulnérabilité de CA du 10 mai 2007 :
<http://supportconnectw.ca.com/public/antivirus/infodocs/caav-secnotice050807.asp>
- Référence CVE CVE-2007-2522 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2522>
- Référence CVE CVE-2007-2523 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2523>

Gestion détaillée du document

11 mai 2007 version initiale.